

AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

FILED  
LODGED  
ENTERED  
RECEIVED

JUL 26 2019

## UNITED STATES DISTRICT COURT

for the

Western District of Washington

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
BY DEPUTY

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)6520 28th Avenue South  
Seattle, Washington

Case No.

MJ19-342

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

6520 28th Avenue South, Seattle, Washington, more fully described in Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*  
 18 U.S.C. § 1030(a)(2) and (5)

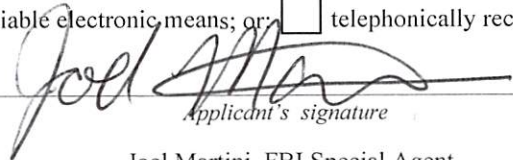
*Offense Description*  
 Computer Fraud/Hacking

The application is based on these facts:

- ☒ See Affidavit of FBI SA Joel Martini, continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

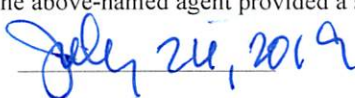
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or ☐ telephonically recorded.

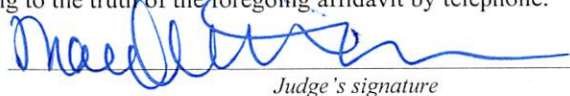
  
 Applicant's signature

Joel Martini, FBI Special Agent  
 Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or  
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date:

  
 July 26, 2019

  
 Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge  
 Printed name and title

STATE OF WASHINGTON           )  
  )           SS  
COUNTY OF KING             )

## I. INTRODUCTION

3. I currently am conducting an investigation of Paige Adele Thompson, also known by the alias “erratic,” for intruding into servers rented or contracted by Capital One Financial Corporation (“Capital One”), a financial services company, from Amazon.com, Inc. (“Amazon”), a company that provides cloud computing services, and for exfiltrating and

1 stealing information, including credit card applications and other documents, from Capital  
2 One.

3 4. I make this affidavit in support of an application for a warrant to search  
4 Thompson's residence, located at 6520 28<sup>th</sup> Avenue South, Seattle, Washington (hereinafter,  
5 "the SUBJECT RESIDENCE"), further described in Attachment A to this Affidavit,  
6 including any computers, cellular telephones, electronic storage media, and other devices  
7 located in that residence, for evidence, fruits, and instrumentalities of computer  
8 fraud/hacking, in violation of Title 18, United States Code § 1030(a)(2) and (5), listed in  
9 Attachment B to this Affidavit.

10 5. The facts set forth in this Affidavit are based on my own personal knowledge,  
11 including interviews I have conducted and my review of documents related to this  
12 investigation; information obtained from other individuals, including other law enforcement  
13 officers and investigators and employees of Capital One; and my training and experience.  
14 Because this Affidavit is submitted for the limited purpose of establishing probable cause in  
15 support of the application for a search warrant, it does not set forth each and every fact that I  
16 or others have learned during the course of this investigation, but rather those relevant to the  
17 determination of whether probable cause exists to issue the requested search warrant.

## 18 II. THE SUBJECT RESIDENCE

19 6. The SUBJECT RESIDENCE is located at 6520 28<sup>th</sup> Avenue South, Seattle,  
20 Washington, and is a grey one-story house with a partial brick facade on the front, and white  
21 window frames and eaves. The number 6520 appears to the right side of the front door. The  
22 SUBJECT RESIDENCE is shown in the photograph in Attachment A, which is attached  
23 hereto and incorporated herein.

## 24 III. SUMMARY OF PROBABLE CAUSE

25 7. The FBI is conducting an investigation into a network intrusion into servers  
26 rented or contracted by Capital One from Amazon. Capital One is a financial services  
27 company that, among other things, issues credit cards. The evidence in this case shows that  
28

1 Thompson, who resides at the SUBJECT RESIDENCE, is the person who committed this  
2 intrusion.

3 8. Evidence linking Thompson to the intrusion includes the fact that information  
4 obtained from the intrusion has been posted on a GitHub page that includes Thompson's full  
5 name – paigeadelethompson – as part of its digital address, and that is linked to other pages  
6 that belong to Thompson and contain her resume. In addition, records obtained from Capital  
7 One indicate that Internet Protocol addresses used by the intruder are controlled by a  
8 company that provides virtual private network services and that was used by Thompson to  
9 make postings on the internet service GitHub, including very close in time to intrusions.  
10 Moreover, Thompson also has made statements on social media fora evidencing the fact that  
11 she has information of Capital One, and that she recognizes that she has acted illegally.

12 9. Thompson resides at the SUBJECT RESIDENCE, and has done so at all times  
13 material to this investigation. As a result, there is probable cause to believe that Thompson  
14 committed some or all of the illegal activity being investigated from the SUBJECT  
15 RESIDENCE, and that evidence of that illegal activity will be found at the SUBJECT  
16 RESIDENCE, including on any computers, cellular telephones, and electronic storage media  
17 that may be found in that residence.

#### 18 IV. TERMS AND DEFINITIONS

19 10. For the purpose of this affidavit, I use the following terms as described below:

20 a. A server is a computer that provides services for other computers  
21 connected to it via a network or the Internet. The computers that use the server's services are  
22 sometimes called clients. Servers can be physically located anywhere with a network  
23 connection that may be reached by the clients. For example, it is not uncommon for a server  
24 to be located hundreds (or even thousands) of miles away from client computers. A server  
25 may be either a physical or virtual machine. A physical server is a piece of computer  
26 hardware configured as a server with its own power source, central processing unit or units,  
27 and associated software. A virtual server typically is one of many servers that operate on a  
28 single physical server. Each virtual server shares the hardware resources of the physical

1 server, but the data residing on each virtual server is segregated from the data on other  
2 virtual servers on the same physical machine.

3           b.     An Internet Protocol address (an "IP address") is a unique numeric  
4 address used by devices, such as computers, on the internet. Every device attached to the  
5 internet is assigned an IP address, so that internet traffic sent from, and directed to, that  
6 device may be directed properly from its source to its destination. Most internet service  
7 providers control a range of IP addresses. Generally, a static IP address is permanently  
8 assigned to a specific location or device, while a dynamic IP address is temporary and  
9 periodically changes.

10           c.     The Onion Router (or "TOR") is an anonymity tool used by individuals  
11 to conceal their identities, including the origin of their internet connection, that is, their IP  
12 addresses. TOR bounces communications through several intermediate computers (relays),  
13 each of which utilizes encryption, thus anonymizing the IP address of the computer of the  
14 individual using TOR.

15           d.     A virtual private network (a "VPN") is a secure connection over a less  
16 secure network, such as the internet. A VPN uses shared public infrastructure, but maintains  
17 privacy through security procedures and tunneling protocols. It encrypts data at the sending  
18 end, decrypts it at the receiving end, and sends the data through a "tunnel" that cannot be  
19 "entered" by data that is not properly encrypted. A VPN also may encrypt the originating  
20 and receiving network addresses.

21           11.    Throughout this Affidavit, I also refer to a number of companies and to  
22 services that they offer:

23           a.     GitHub is a company that provides webhosting and allows users to  
24 manage and store revisions of projects. Although used mostly for software development  
25 projects, GitHub also allows users to manage other types of files.

26           b.     IPredator is a company that offers prepaid VPN service to customers,  
27 using servers based in Sweden.



1 c. Meetup is an Internet-based platform designed to let people find and  
2 build local communities, called “groups.”

3 d. Slack is a cloud-based set of team-collaboration software tools and  
4 online services. Slack allows users to establish “channels,” in which a team can share  
5 messages, tools, and files.

6 e. Twitter is company that operates a social networking site that allows  
7 users to establish accounts, post short messages, and receive other users’ messages.

## 8 V. THE INVESTIGATION

### 9 A. The Intrusion and Exfiltration

10 12. Capital One is a financial services company that offers, among other products,  
11 credit cards. Capital One maintains an e-mail address through which it solicits disclosures of  
12 actual or potential vulnerabilities in its computer systems, so that Capital One can learn of,  
13 and attempt to avert, breaches of its systems. Among others who send e-mails to this address  
14 are individuals who sometimes are called “ethical” or “white hat” hackers. Like other  
15 companies, Capital One often will make payments to individuals who provide information  
16 concerning actual or potential vulnerabilities.

17 13. On July 17, 2019, an individual – who previously was unknown to Capital One  
18 - emailed this e-mail address. The individual’s e-mail stated that there appeared to be leaked  
19 data belonging to Capital One on GitHub, and provided the address of the GitHub file  
20 containing this leaked data. The address provided for this file was  
21 [https://gist.github.com/paigeadelethompson/\\*\\*\\*\\*\\*](https://gist.github.com/paigeadelethompson/*****). [Throughout this affidavit, I use \*\*\*\*\*  
22 to substitute for other characters, often more than five characters.] Significantly, this address  
23 includes the name paigeadelethompson, which I know to be Thompson’s full name. The  
24 individual providing this information offered to help track down the person who had posted  
25 this information. The individual providing the information also subsequently has indicated  
26 that he/she hopes to be paid for providing the information.

27 14. After receiving this information, Capital One examined the GitHub file, which  
28 was timestamped April 21, 2019 (the “April 21 File”). Capital One determined that the April

1 21 File contained the IP address for a server rented or contracted by Capital One from  
2 Amazon, and the number of a port on that server that had been misconfigured, with the result  
3 that commands addressed to that IP address and port passed through directly to the server.

4 15. Capital One determined that the April 21 File contained code for three  
5 commands, as well as a list of more than 700 folders or buckets of data.

6 ■ Capital One determined that the first command (which was directed at the  
7 misconfigured port), when executed, obtained security credentials for an  
8 account known as ISRM-WAF-Role that, in turn, enabled access to certain  
9 of Capital One's folders or buckets of data at Amazon.

10 ■ Capital One determined that the second command (the "List Buckets  
11 Command"), when executed, used the ISRM-WAF-Role account to list the  
12 names of folders or buckets of data in Capital One's storage space at  
13 Amazon.

14 ■ Capital One determined that the third command (the "Sync Command"),  
15 when executed, used the ISRM-WAF-Role to extract or copy data from  
16 those folders or buckets in Capital One's storage space for which the  
17 ISRM-WAF-Role account had the requisite permissions.

18 16. Capital One tested the commands in the April 21 File, and confirmed that the  
19 commands did, in fact, function to obtain Capital One's credentials, to list or enumerate  
20 folders or buckets of data, and to extract data from certain of those folders or buckets.  
21 Capital One confirmed that the more-than-700 folders or buckets of data listed in the April  
22 21 File matched the actual names of folders or buckets of data used by Capital One for data  
23 stored at Amazon. Capital One report that its computer logs reflect the fact that the List  
24 Buckets Command was in fact executed on April 21, 2019, and that the timestamp in Capital  
25 One's logs matches the timestamp in the April 21 File.

26 17. According to Capital One, its logs show a number of connections or attempted  
27 connections to Capital One's server from TOR exit nodes, and a number of connections from  
28 IP addresses beginning with 46.246, all of which Capital One believes relate to activity

1 conducted by the same person involved in the April 21, 2019, intrusion, because they involve  
2 unusual communications with the same misconfigured port discussed above. Specifically,  
3 according to Capital One, the logs show:

- 4 ■ On or about March 12, 2019, IP address 46.246.35.99 attempted to access  
5 Capital One's data. I know, from checking publicly-available records, that  
6 this IP address is controlled by IPredator, a company that provides VPN  
7 services.
- 8 ■ On or about March 22, 2019, the ISRM-WAF-Role account was used to  
9 execute the List Buckets Command several times. These commands were  
10 executed from IP addresses that I believe to be TOR exit nodes. According  
11 to Capital One, the ISRM-WAF-Role account does not, in the ordinary  
12 course of business, invoke the List Buckets Command.
- 13 ■ Also on or about March 22, 2019, the ISRM-WAF-Role account was used  
14 to execute the Sync Command a number of times to obtain data from  
15 certain of Capital One's data folders or buckets. A number of those  
16 commands were executed from IP address 46.246.38.224. I know, from  
17 checking publicly-available records, that that IP address also is controlled  
18 by IPredator.
- 19 ■ One of the files copied from Capital One's folders or buckets on March 22,  
20 2019, was a file with the name \*\*\*\*\*c000.snappy.parquet (the "Snappy  
21 Parquet File"), and this was the only time the ISRM-WAF-Role account  
22 accessed the Snappy Parquet File between January 1, 2019 and July 20,  
23 2019.
- 24 ■ A List Buckets Command was executed on April 21, 2019, from IP address  
25 46.246.35.103. I know, from checking publicly-available records, that the  
26 IP address from which this command was executed also is controlled by  
27 IPredator. I also believe, based on the timestamp on the April 21, 2019 file,  
28 and the time that Capital One reports that the command appears in Capital



1           One's logs, that this was the command that was the source of the April 21  
2           File.

3           18.       According to Capital One, the data copied from Capital One's data folders or  
4 buckets includes primarily credit card applications. Although some of the information in  
5 those applications (such as Social Security numbers) has been tokenized or encrypted, other  
6 information including applicants' names, addresses, dates of birth and information regarding  
7 their credit history has not been tokenized. According to Capital One, the data includes large  
8 numbers of applications, possibly tens of millions of applications. In addition, according to  
9 Capital One, the data includes several hundred thousand applications that include tax returns,  
10 including social security numbers, or applicants' income and partial social security numbers,  
11 and also includes more than 100,000 records that include bank account information.

12 **B.     Evidence of Thompson's Involvement**

13           19.       As noted above, the GitHub address for the April 21 File includes the name  
14 paigeadelethompson. Clicking on the name paigeadelethompson in the address takes the  
15 user to the main GitHub page for a Paige Adele Thompson. The profile on that page  
16 contains a link to a GitLab page at [www.gitlab.com/netcrave](http://www.gitlab.com/netcrave) (the "GitLab Netcrave Page").  
17 The GitLab Netcrave Page includes, among other things, a resume for a "Paige Thompson."  
18 That resume indicates that Thompson is a "systems engineer" and formerly worked at  
19 Amazon from 2015-16. The resume also lists an address of 6520 28th Avenue South,  
20 Seattle, Washington, the address of the SUBJECT RESIDENCE. Based on this evidence, I  
21 believe that Thompson is the user of the GitHub and GitLab accounts described herein.

22           20.       An April 19, 2019, post in the GitHub account of "paigeadelethompson"  
23 includes a "Server List" of IP addresses associated with the account. All of the IP addresses  
24 in the Server List begin with 46.246. I have confirmed by checking publicly-available  
25 records that each of the IP addresses in the "Server List" is controlled by IPredator. (As  
26 noted above, Capital One reports that its logs reveal malicious activity, including malicious  
27 activity on April 19, 2019, that, similarly, comes from several IP addresses beginning with  
28

1 46.246 that, based on publicly available records, are associated with the VPN service  
2 IPredator.)

3 21. Based on open source research, I am aware of a Meetup group called "Seattle  
4 Warez Kiddies" with a Web page located at [www.meetup.com/Seattle-Warez-Kiddies](http://www.meetup.com/Seattle-Warez-Kiddies). That  
5 page indicates that its organizer is "Paige Thompson (erratic)." Within that Meetup group is  
6 a Slack invitation code for the Slack channel netcrave.slack.com (the "Netcrave Slack  
7 Channel").

8 22. I have reviewed postings on the Netcrave Slack Channel. Among other things,  
9 on or about June 26, 2019, a user "erratic" posted a list of files that "erratic" claimed to  
10 possess. Among those files, two referenced "ISRM-WAF-Role." Based on my review of  
11 the Sync Command in the April 21 File, and my training and experience, I know that the  
12 Sync Command would place extracted files in a directory with the name "ISRM-  
13 WAF-Role." Accordingly, I believe that, "erratic" was claiming to have files extracted using  
14 the extraction command set forth in the April 21 File.

15 23. On or about June 27, 2019, "erratic" posted about several companies,  
16 government entities, and educational institutions. Among these posts, "erratic" referred to  
17 "ISRM-WAF-Webrole" and indicated that account was associated with Capital One. Based  
18 on my training and experience, these communications appear to be references by "erratic" to  
19 other intrusions that "erratic" may have committed.

20 24. On or about June 27, 2019, another user posted "don't go to jail plz." In  
21 response, "erratic" posted "Im like > ipredator > tor > s3 on all this shit." I understand this  
22 to refer to the method Thompson used to commit the intrusion. "[E]rratic" also posted "I  
23 wanna get it off my server that's why Im archiving all of it lol."

24 25. According to a screenshot that Capital One provided, and that I have  
25 reviewed, on or about June 27, 2019, the user "paigeadele" posted, "I've also got a leak  
26 proof IPredator router setup if anyone neds [sic] it," as well as a GitHub link that included  
27 "paigeadelethompson" in the link. I was not able to locate this post on GitHub myself,  
28 although that may be because it since has been deleted.

1       26. According to a screenshot that Capital One provided, and that I have reviewed,  
2 on or about July 4, 2019, the user "paigeadele" posted a message seeking information about  
3 the Snappy Parquet File, one of the files exfiltrated from Capital One on March 22, 2019.

4       27. On or about July 19, 2019, the user "paigeadele" posted information about one  
5 of her pets. Included in the post was an estimate from a veterinarian dated June 10, 2019,  
6 provided to "Paige Thompson" at the address 6520 28th Avenue South, Seattle Washington,  
7 the address of the SUBJECT RESIDENCE. Based upon the information in the preceding  
8 paragraphs, I believe that Thompson is the person who poste under the names "erratic" and  
9 "paigeadele" on the Netcrave Slack Channel.

10       28. I have learned, from Capital One and through open-source research, of a  
11 Twitter account name @0xA3A97B6C, with a username "ERRATIC." I have reviewed  
12 photographs posted to the account of "ERRATIC," and they appear to depict the same  
13 individual who appears in photographs posted on the Netcrave Slack Channel under the  
14 username "paigeadele. I believe that Thompson is the user of the "ERRATIC" Twitter  
15 account.

16       29. According to a screenshot that Capital One provided, and that I have reviewed,  
17 on June 18, 2019, "ERRATIC" posted "Ive basically strapped myself with a bomb vest,  
18 fucking dropping capitol ones dox and admitting it. I wanna distribute those buckets i think  
19 first." I understand this post to indicate, among other things, that Thompson intended to  
20 disseminate data stolen from victim entities, starting with Capital One.

21 **C. Evidence that Thompson lives at the SUBJECT RESIDENCE**

22       30. As noted above, Thompson's resume on the GitLab Netcrave Page lists  
23 Thompson's address as being the SUBJECT RESIDENCE. In addition, a veterinarian's bill  
24 sent to her on June 10, 2019, was addressed to her at the SUBJECT RESIDENCE.

25       31. I also have reviewed a Seattle Police Department report dated March 24, 2019,  
26 that shows that officers responded to the SUBJECT RESIDENCE. That report was  
27 classified as a response to "suicide-threats." The report listed three people as living at the  
28 SUBJECT RESIDENCE, Thompson, P.Q., and J.E. One of the other residents told officers

1 that Thompson had threatened her, and that Thompson previously has threatened to commit  
2 “suicide by cop.” Thompson explained her conduct by stating that she was upset that  
3 something had gone wrong with her computer.

4 32. According to land records, P.Q. is the owner of the SUBJECT RESIDENCE. I  
5 have conducted surveillance at the SUBJECT RESIDENCE. During the course of that  
6 surveillance, I observed three vehicles (which are shown in the picture in Attachment A) at  
7 the SUBJECT RESIDENCE. All three of these vehicles are registered to P.Q.

8 33. Multiple law enforcement officers, including myself, have conducted physical  
9 surveillance at the SUBJECT RESIDENCE. On July 26, 2019, surveillance observed  
10 Thompson as well as two others, believed to be P.Q. and J.E., at the SUBJECT  
11 RESIDENCE.

12 34. Based on this information, I believe that Thompson currently lives at the  
13 SUBJECT RESIDENCE. (Although Thompson’s Department of Licensing Record lists her  
14 at a different address in Seattle, that listing was last updated on August 31, 2018, and I  
15 believe that it is out of date.)

16 35. I am not aware of any evidence that Thompson currently is employed. (Her  
17 resume shows her last employment, at Amazon, as ending in 2016.) As a result, I believe  
18 that any computers, and electronic storage media belonging to Thompson are likely also to  
19 be found at that address.

20 **VI. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

21 36. As described above and in Attachment B, this application seeks permission to  
22 search for evidence, fruits, and instrumentalities that might be found at the SUBJECT  
23 RESIDENCE, in whatever form they are found. One form in which they might be found is  
24 data stored on digital devices,<sup>1</sup> such as computers and cellular telephones, and electronic  
25

26 <sup>1</sup> “Digital device” includes any device capable of processing and/or storing data in electronic  
27 form, including, but not limited to: computer servers, central processing units, laptop,  
28 desktop, notebook and tablet computers, drives intended for removable media, related  
communications devices such as modems, routers, and switches, wireless communication  
devices such as cellular telephones, and iPods/iPads.

1 storage media.<sup>2</sup> Thus, the warrant applied for would authorize the seizure of digital devices  
 2 and electronic storage media and, potentially, the copying of electronically stored  
 3 information from digital devices or electronic storage media, under Rule 41(e)(2)(B).

4 37. *Probable cause.* Based upon my review of the evidence gathered in this  
 5 investigation, my review of data and records, information received from other agents and  
 6 computer forensics examiners, and my training and experience, I submit that, if a digital  
 7 device or other electronic storage media is found at the SUBJECT RESIDENCE, there is  
 8 probable cause to believe that evidence, fruits, and instrumentalities of the crime of computer  
 9 hacking will be stored on those digital devices and other electronic storage media. I believe  
 10 this because the intrusion under investigation was committed through the use of digital  
 11 devices, and because information stolen from Capital One has been received by digital  
 12 devices. Both the intrusion, and the storage of the resulting information, will have resulted  
 13 in evidence on those digital devices or electronic storage media:

- 14 a. Based on my knowledge, training, and experience, I know that computer files  
 15 or remnants of such files can be preserved (and consequently also then  
 16 recovered) for months or even years after they have been downloaded onto a  
 17 storage medium, deleted, or accessed or viewed via the Internet. Electronic  
 18 files downloaded to a digital device or other electronic storage medium can be  
 19 stored for years at little or no cost. Even when files have been deleted, they  
 20 can be recovered months or years later using forensic tools. This is so because,  
 when a person “deletes” a file on a digital device or other electronic storage  
 media, the data contained in the file does not actually disappear; rather, that  
 data remains on the storage medium until it is overwritten by new data.
- 21 b. Therefore, deleted files, or remnants of deleted files, may reside in free space  
 22 or slack space—that is, in space on the digital device or other electronic  
 23 storage medium that is not currently being used by an active file—for long  
 24 periods of time before they are overwritten. In addition, a computer’s  
 operating system may also keep a record of deleted data in a “swap” or  
 “recovery” file.

25  
 26  
 27 <sup>2</sup> Electronic Storage media is any physical object upon which electronically stored  
 28 information can be recorded. Examples include hard disks, RAM, floppy disks, flash  
 memory, CD-ROMs, and other magnetic or optical media.



- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the SUBJECT RESIDENCE because:

- a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude

the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.<sup>1</sup> Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence

---

<sup>1</sup> For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

## **VII. DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES**

39. In this case, the evidence suggests that digital devices also been used as instrumentalities of the crime being investigated. Specifically, the intrusion under investigation was committed through the use of digital devices, and the information stolen from Capital One has been received by digital devices. Indeed, the crime being investigated could not have been committed without using digital devices.

## **VIII. PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION**

40. Because of the nature of the evidence that I am attempting to obtain and the nature of the investigation, I have not made any prior efforts to obtain the evidence based on the consent of any party who may have authority to consent. Indeed, I am concerned that if Thompson becomes aware of the investigation in advance of the execution of a search

1 warrant, she may either (1) attempt to destroy any potential evidence, whether digital or non-  
2 digital, thereby hindering law enforcement agents from the furtherance of the criminal  
3 investigation, or (2) reveal sensitive financial and other personal information stolen from  
4 Capital One.

5 **IX. RISK OF DESTRUCTION OF EVIDENCE**

6 41. I know based on my training and experience that digital information can be  
7 very fragile and easily destroyed. Digital information can also be easily encrypted or  
8 obfuscated such that review of the evidence would be extremely difficult, and in some cases  
9 impossible. If an encrypted computer is either powered off or if the user has not entered the  
10 encryption password and logged onto the computer, it is likely that any information  
11 contained on the computer will be impossible to decipher. If the computer is powered on,  
12 however, and the user is already logged onto the computer, there is a much greater chance  
13 that the digital information can be extracted from the computer. This is because when the  
14 computer is on and in use, the password has already been entered and the data on the  
15 computer is accessible. However, giving the owner of the computer time to activate a digital  
16 security measure, pull the power cord from the computer, or even log off of the computer  
17 could result in a loss of digital information that could otherwise have been extracted from the  
18 computer.

19 **X. REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH**

20 42. *Necessity of seizing or copying entire computers or storage media.* In most  
21 cases, a thorough search of premises for information that might be stored on digital devices  
22 or other electronic storage media requires the seizure of the physical items and later off-site  
23 review consistent with the warrant. In lieu of removing all of these items from the premises,  
24 it is sometimes possible to make an image copy of the data on the digital devices or other  
25 electronic storage media, onsite. Generally speaking, imaging is the taking of a complete  
26 electronic picture of the device's data, including all hidden sectors and deleted files. Either  
27 seizure or imaging is often necessary to ensure the accuracy and completeness of data  
28

1 recorded on the item, and to prevent the loss of the data either from accidental or intentional  
2 destruction. This is true because of the following:

- 3 a. *The time required for an examination.* As noted above, not all evidence takes  
4 the form of documents and files that can be easily viewed on site. Analyzing  
5 evidence of how a computer has been used, what it has been used for, and who  
6 has used it requires considerable time, and taking that much time on premises  
7 could be unreasonable. As explained above, because the warrant calls for  
8 forensic electronic evidence, it is exceedingly likely that it will be necessary to  
9 thoroughly examine the respective digital device and/or electronic storage  
10 media to obtain evidence. Computer hard drives, digital devices and electronic  
11 storage media can store a large volume of information. Reviewing that  
12 information for things described in the warrant can take weeks or months,  
13 depending on the volume of data stored, and would be impractical and invasive  
14 to attempt on-site.
- 15 b. *Technical requirements.* Digital devices or other electronic storage media can  
16 be configured in several different ways, featuring a variety of different  
17 operating systems, application software, and configurations. Therefore,  
18 searching them sometimes requires tools or knowledge that might not be  
19 present on the search site. The vast array of computer hardware and software  
20 available makes it difficult to know before a search what tools or knowledge  
21 will be required to analyze the system and its data on the premises. However,  
22 taking the items off-site and reviewing them in a controlled environment will  
23 allow examination with the proper tools and knowledge.
- 24 c. *Variety of forms of electronic media.* Records sought under this warrant could  
25 be stored in a variety of electronic storage media formats and on a variety of  
26 digital devices that may require off-site reviewing with specialized forensic  
27 tools.

## 21 **XI. SEARCH TECHNIQUES**

22 43. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal  
23 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or  
24 otherwise copying digital devices and other electronic storage media that reasonably appear  
25 capable of containing some or all of the data or items that fall within the scope of  
26 Attachment B to this Affidavit, and will specifically authorize a later review of the media or  
27 information consistent with the warrant.  
28



1 44. Because several people share the SUBJECT RESIDENCE as a residence, it is  
2 possible that the SUBJECT RESIDENCE will contain digital devices or other electronic  
3 storage media that are predominantly used, and perhaps owned, by persons who are not  
4 suspected of a crime. If agents conclude that any digital device or other electronic storage  
5 media is owned, and predominantly used, by a person other than Thompson, agents will  
6 seize, but will not conduct any further search of, that digital device or other electronic  
7 storage media. It may be impossible to determine, on scene, which computers contain the  
8 things described in this warrant.

9 45. Consistent with the above, I hereby request the Court's permission to seize  
10 and/or obtain a forensic image of digital devices or other electronic storage media that  
11 reasonably appear capable of containing data or items that fall within the scope of  
12 Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other  
13 electronic storage media and/or forensic images, using the following procedures:

14 **A. Processing the Search Sites and Securing the Data.**

- 15 a. Upon securing the physical search site, the search team will conduct an initial  
16 review of any digital devices or other electronic storage media located at the  
17 subject premises described in Attachment A that are capable of containing data  
18 or items that fall within the scope of Attachment B to this Affidavit, to  
19 determine if it is possible to secure the data contained on these devices onsite  
20 in a reasonable amount of time and without jeopardizing the ability to  
21 accurately preserve the data.
- 22 b. In order to examine the electronically stored information ("ESI") in a  
23 forensically sound manner, law enforcement personnel with appropriate  
24 expertise will attempt to produce a complete forensic image, if possible and  
25 appropriate, of any digital device or other electronic storage media that is  
26 capable of containing data or items that fall within the scope of Attachment B  
27 to this Affidavit.<sup>1</sup>

28 <sup>1</sup> The purpose of using specially trained computer forensic examiners to conduct the imaging  
of digital devices or other electronic storage media is to ensure the integrity of the evidence  
and to follow proper, forensically sound, scientific procedures. When the investigative agent  
is a trained computer forensic examiner, it is not always necessary to separate these duties.  
Computer forensic examiners often work closely with investigative personnel to assist  
investigators in their search for digital evidence. Computer forensic examiners are needed  
because they generally have technological expertise that investigative agents do not possess.

- 1 c. A forensic image may be created of either a physical drive or a logical drive.  
2 A physical drive is the actual physical hard drive that may be found in a typical  
3 computer. When law enforcement creates a forensic image of a physical drive,  
4 the image will contain every bit and byte on the physical drive. A logical  
5 drive, also known as a partition, is a dedicated area on a physical drive that  
6 may have a drive letter assigned (for example the c: and d: drives on a  
7 computer that actually contains only one physical hard drive). Therefore,  
8 creating an image of a logical drive does not include every bit and byte on the  
9 physical drive. Law enforcement will only create an image of physical or  
10 logical drives physically present on or within the subject device. Creating an  
11 image of the devices located at the search locations described in Attachment A  
12 will not result in access to any data physically located elsewhere. However,  
13 digital devices or other electronic storage media at the search locations  
14 described in Attachment A that have previously connected to devices at other  
15 locations may contain data from those other locations.  
16
- 17 d. If based on their training and experience, and the resources available to them at  
18 the search site, the search team determines it is not practical to make an on-site  
19 image within a reasonable amount of time and without jeopardizing the ability  
20 to accurately preserve the data, then the digital devices or other electronic  
21 storage media will be seized and transported to an appropriate law enforcement  
22 laboratory to be forensically imaged and reviewed.

17 **B. Searching the Forensic Images.**

- 18 a. Searching the forensic images for the items described in Attachment B may  
19 require a range of data analysis techniques. In some cases, it is possible for  
20 agents and analysts to conduct carefully targeted searches that can locate  
21 evidence without requiring a time-consuming manual search through unrelated  
22 materials that may be commingled with criminal evidence. In other cases,  
23 however, such techniques may not yield the evidence described in the warrant,  
24 and law enforcement may need to conduct more extensive searches to locate  
25 evidence that falls within the scope of the warrant. The search techniques that  
26 will be used will be only those methodologies, techniques and protocols as  
27 may reasonably be expected to find, identify, segregate and/or duplicate the  
28 items authorized to be seized pursuant to Attachment B to this affidavit. Those  
29 techniques, however, may necessarily expose many or all parts of a hard drive

Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

1 to human inspection in order to determine whether it contains evidence  
2 described by the warrant.

- 3 b. Agents may utilize hash values to exclude certain known files, such as the  
4 operating system and other routine software, from the search results. However,  
5 because the evidence I am seeking does not have particular known hash values,  
6 agents will not be able to use any type of hash value library to locate the items  
7 identified in Attachment B.

## 8 **XII. FORFEITURE**

9 46. This application requests the issuance of a warrant under 21 U.S.C. § 853(f)  
10 authorizing the seizure of property subject to forfeiture. This is appropriate because:  
11 (1) there is probable cause to believe that the property to be seized would, in the event of  
12 conviction, be subject to forfeiture, and (2) an order under 21 U.S.C. § 853(e) may not be  
13 sufficient to assure the availability of the property for forfeiture. There is probable cause to  
14 believe that the property to be seized would, in the event of conviction, be subject to  
15 forfeiture, because 18 U.S.C. § 1030(i)(1)(A) provides that the defendant's "interest in any  
16 personal property that was used or intended to be used to commit or to facilitate the  
17 commission of such violation" shall be forfeited to the United States.

18 //

19 //

20 //

**XIII. CONCLUSION**

47. For the reasons set forth above, there is probable cause to believe that evidence, fruits and/or instrumentalities of computer fraud/hacking, in violation of Title 18, United States Code § 1030(a)(2) and (5), are located in the SUBJECT RESIDENCE, as more fully described in Attachment A to this Affidavit, including on any computers, cellular telephones, and electronic storage media that may be found in the SUBJECT RESIDENCE. I therefore request that the court issue a warrant authorizing a search of SUBJECT RESIDENCE for the items more fully described in Attachment B hereto, and the seizure of any such items found therein.

  
JOEL MARTINI  
Special Agent  
Federal Bureau of Investigation

SUBSCRIBED AND SWORN before me this 26 day of July, 2019.

  
MARY ALICE THEILER  
United States Magistrate Judge



**ATTACHMENT A**  
**LOCATION TO BE SEARCHED**

The SUBJECT RESIDENCE, depicted in the photograph below, is located at 6520 28th Avenue South, Seattle, Washington, and is a grey one-story house with a partial brick facade on the front, and white window frames and eaves. The number 6520 appears to the right side of the front door.





**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 1030(a)(2) and (5) for the period from January 1, 2019, to the present:

1. All records relating to any intrusion into servers rented, leased, or contracted by Capital One Financial Corporation (“Capital One”) from Amazon.com, Inc. (“Amazon”), or to the exfiltration or theft of data from such servers.
2. All records (including file structures as well as credit card applications, tax returns and bank account information) exfiltrated or stolen from Capital One.
3. All credit card applications, tax returns and bank account information of any person other than (a) Paige Thompson, (b) any other resident of the SUBJECT RESIDENCE, or (c) any family member of either Paige Thompson or any other resident of the SUBJECT RESIDENCE.
4. All records relating to the use of a GitHub account in the name paigadelethompson.
5. All records relating to the use of IPredator or the TOR network.
6. All records evidencing the use of the nickname or identity “paigadelethompson.”
7. All records relating to the use or, or access to the following services: Twitter, Slack, GitLab, and Meetup.
8. All records evidencing the use of the nickname or identity “erratic.”
9. All records relating to Capital One.

10. All records relating to Amazon, including to any prior employment at Amazon.
11. All records relating to any intrusion into the servers of any company, educational institution, or governmental entity, at Amazon or elsewhere, or to the exfiltration or theft of data from such servers.
12. All computers, notebook computers, laptop computers, and electronic storage media and/or their components, which include:
  - a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;
  - b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;
  - c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
  - d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;
  - e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
  - f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
  - g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.
13. Any digital devices or electronic storage media that were or may have been used as a means to commit the offenses described on the warrant, including computer fraud/hacking in violation of 18 U.S.C. § 1030(a)(2) and (5).
14. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be

contained, or that may contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
  - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
  - f. evidence of the times the digital device or other electronic storage media was used;
  - g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;
  - h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media; and
  - i. contextual information necessary to understand the evidence described in this attachment.
15. Records and things evidencing communication with an Internet Protocol address controlled by IPredator or with the TOR network:
- a. routers, modems, and network equipment used to connect computers to the Internet;
  - b. records of Internet Protocol addresses used and connected to;
  - c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the

user entered into any Internet search engine, and records of user-typed web addresses.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

THIS WARRANT AUTHORIZES THE SEIZURE OF DIGITAL DEVICES AND OTHER ELECTRONIC STORAGE MEDIA FOUND IN THE SUBJECT RESIDENCE THAT APPEAR TO BE OWNED, AND PREDOMINANTLY USED, BY A PERSON OTHER THAN PAIGE THOMPSON, BUT IT DOES NOT AUTHORIZE THE FURTHER SEARCH OF THOSE DEVICES (WHICH SHALL REQUIRE THE ISSUANCE OF A FURTHER SEARCH WARRANT AUTHORIZING SUCH ACTUAL SEARCH).